SPYWOLF

Security Audit Report

Audit prepared for

Blastex

Completed on

March 20, 2024

KEY RESULTS

Cannot mint new tokens	**
Cannot pause trading (honeypot)	*
Cannot blacklist an address	Passed
Cannot raise taxes over 25%?	Passed
No proxy contract detected	Passed
Not required to enable trading	*
No hidden ownership	Passed
Cannot change the router	Passed
No cooldown feature found	Passed
Bot protection delay is lower than 5 blocks	Passed
Cannot set max tx amount below 0.05% of total supply	Passed
The contract cannot be self-destructed by owner	Passed

For a more detailed and thorough examination of the heightened risks, refer to the subsequent parts of the report.

*Only new deposits/reinvestments can be paused

**New tokens can be minted only via the staking contract's bonding mechanism

OVERVIEW

This goal of this report is to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team’s evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

Blastex

PROJECT DESCRIPTION

According to their website:

Blastex is a disruptive Ethereum staking protocol that leverages the Blast native ETH yield, gas sharing, and Blast Points to lead the passive income revolution along with its community.

Make your ETH work for you on multiple levels while farming Blast Points yields and Blast Points.

Release Date: Launching in March, 2024

Category: Staking

CONTRACT INFO

Token Name
N/A

Symbol
N/A

Contract Address
0x8C1DBB14c012bCCdB3477bc1625A3DCfD0F61ac2

Network
Blast

Language
Solidity

Deployment Date
March 19, 2024

Contract Type
Staking

Total Supply
N/A

Status
Not launched

TAXES

Buy Tax
10%

Sell Tax
n/a

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	N/A
Uniq Senders	N/A
Uniq Receivers	N/A
Total Amount	N/A
Median Transfer Amount	N/A
Average Transfer Amount	N/A
First transfer date	N/A
Last transfer date	N/A
Days token transferred	N/A

SMART CONTRACT STATS

Calls Count	N/A
External calls	N/A
Internal calls	N/A
Transactions count	N/A
Uniq Callers	N/A
Days contract called	N/A
Last transaction time	Mar-19-2024 05:10:29 PM +UTC
Created	Mar-19-2024 05:08:45 PM +UTC
Create TX	0x5e554dd702fd7ee698b355755b65006b12e70958a99dd9e2c8fec98c9130c933
Creator	0x6d9725ffec14648300bc7bc6c9c0dd5ea631b39e

VULNERABILITY ANALYSIS

ID	Title	
SWC-100	Function Default Visibility	**Passed**
SWC-101	Integer Overflow and Underflow	**Passed**
SWC-102	Outdated Compiler Version	**Passed**
SWC-103	Floating Pragma	**Passed**
SWC-104	Unchecked Call Return Value	**Passed**
SWC-105	Unprotected Ether Withdrawal	**Passed**
SWC-106	Unprotected SELFDESTRUCT Instruction	**Passed**
SWC-107	Reentrancy	**Passed**
SWC-108	State Variable Default Visibility	**Passed**
SWC-109	Uninitialized Storage Pointer	**Passed**
SWC-110	Assert Violation	**Passed**
SWC-111	Use of Deprecated Solidity Functions	**Passed**
SWC-112	Delegatecall to Untrusted Callee	**Passed**
SWC-113	DoS with Failed Call	**Passed**
SWC-114	Transaction Order Dependence	**Passed**
SWC-115	Authorization through tx.origin	**Passed**
SWC-116	Block values as a proxy for time	**Passed**
SWC-117	Signature Malleability	**Passed**
SWC-118	Incorrect Constructor Name	**Passed**

VULNERABILITY ANALYSIS

ID	Title	
SWC-119	Shadowing State Variables	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed
SWC-122	Lack of Proper Signature Verification	Passed
SWC-123	Requirement Violation	Passed
SWC-124	Write to Arbitrary Storage Location	Passed
SWC-125	Incorrect Inheritance Order	Passed
SWC-126	Insufficient Gas Griefing	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed
SWC-128	DoS With Block Gas Limit	Passed
SWC-129	Typographical Error	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed
SWC-131	Presence of unused variables	Passed
SWC-132	Unexpected Ether balance	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed
SWC-134	Message call with hardcoded gas amount	Passed
SWC-135	Code With No Effects	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed

VULNERABILITY ANALYSIS

NO ERRORS FOUND

MANUAL
CODE REVIEW

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time.

We categorize these vulnerabilities by 4 different threat levels.

THREAT LEVELS

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance, functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium Risk

Administrators can create new bond for user, up to contract's current token balances.

```
function influencerBond(
    address userAddr, uint256 tokensAmount,
    address upline) external onlyModerator {
    require(tokensAmount > 1e18, "M04");
    require(!userAddr.isContract(), "X");
    require(userAddr != upline, "M03");
    require(users[userAddr].bondsNumber < Constants.BONDS_LIMIT, "01");
    require(IERC20(address(token)).balanceOf(address(this)) >= tokensAmount,
    "Insufficient token balance");
    if (upline == address(0x0)) {
      upline = DEFAULT_UPLINE;
    }
    if (users[userAddr].upline == address(0x0)) {
      users[userAddr].upline = upline;
      if (users[userAddr].lastActionTime == 0) {
        users[userAddr].lastActionTime = block.timestamp;
      }

      users[upline].referrals.push(userAddr);
      for (uint256 i = 0; i < REFERRAL_DEPTH; i++) {
        users[upline].refsNumber[i]++;
        upline = users[upline].upline;

        if (upline == address(0x0)) {
          break;
        }
      }

      emit Events.NewUser(
        userAddr, upline, block.timestamp
      );
    }

    uint256 ethAmount = getETHAmount(tokensAmount);
    uint8 bondIdx = newBond(userAddr, 4, ethAmount, 0);

    token.burn(tokensAmount);

    emit Events.NewBond(
      userAddr, 4, bondIdx, ethAmount, tokensAmount, false, block.timestamp
    );
}
```

- Recommendation:
  - No bonds should be issued for free

FOUND THREATS

Informational

Owner can pause only new buys before the launch of platform.

```
function pause() external onlyOwner {
    _pause();
}
```

Owner can activate/deactivate short bonds 1 to 3.
Bonds 0 (for 30 days) cannot be deactivated.

```
bool[5] public BOND_ACTIVATIONS = [
    true,
    false,
    false,
    false,
    false
];

function activateBondType(uint8 bondType) external onlyOwner {
    require(bondType > 0 && bondType < 4, "U1");
    BOND_ACTIVATIONS[bondType] = true;
}

function deactivateBondType(uint8 bondType) external onlyOwner {
    require(bondType > 0 && bondType < 4, "U1");
    BOND_ACTIVATIONS[bondType] = false;
}
```

FOUND THREATS

Informational

Moderator can change tokens claim rate settings.

```
function newPeriod(
    uint256 distributionPercent,
    uint256 contributionDecreasePercent
  ) external onlyModerator {
    require(
        (distributionPercent >= 50 && distributionPercent <= 500)
      || (periodsNumber > 0 && distributionPercent == 0),
      "M00"
    );
    require(
        (contributionDecreasePercent >= 100 && contributionDecreasePercent <= 2000)
      || (periodsNumber > 0 && contributionDecreasePercent == 0),
      "M01"
    );

    require(
      periodsNumber == 0 || lastPeriodIsClosed(),
      "M02"
    );

    if (periodsNumber > 0 && periods[periodsNumber - 1].tvl == 0) {
      (periods[periodsNumber - 1].tvl, ) = getTokenLiquidity();
    }

    periods[periodsNumber] = Models.Period({
      tvl: 0,
      distributionPercent: distributionPercent > 0
        ? distributionPercent
        : periods[periodsNumber - 1].distributionPercent,
      contributionDecreasePercent: contributionDecreasePercent > 0
        ? contributionDecreasePercent
        : periods[periodsNumber - 1].contributionDecreasePercent,
      startTime: block.timestamp
    });

    periodsNumber++;
}
```

FOUND THREATS

Informational

Users can rebond their bonds on behalf of another user.

```
function rebond(uint256 tokensAmount, address receiver) external notContract {
    require(!receiver.isContract(), "20");
    if (receiver == address(0x0)) {
      receiver = msg.sender;
    }
    require(users[receiver].lastActionTime > 0, "21");

    require(users[receiver].bondsNumber < Constants.BONDS_LIMIT, "22");
    require(tokensAmount >= Constants.MIN_BOND_TOKENS, "23");
    require(userBalance(msg.sender) >= tokensAmount, "24");

    collect(msg.sender);
    Models.User storage user = users[msg.sender];
    require(user.balance >= tokensAmount, "24");

    user.balance-= tokensAmount;

    uint256 ethAmount = getETHAmount(tokensAmount);
    uint8 bondIdx = newBond(receiver, 0, ethAmount, 0);

    emit Events.ReBond(
      receiver, bondIdx, ethAmount, tokensAmount, block.timestamp
    );
}
```

FOUND THREATS

Informational

Owner can withdraw any tokens from the contract except the native BLASTEX token and LP token.

```
function retrieveERC20(address tokenAddress, uint256 amount) external onlyOwner {
    require(
      tokenAddress != address(token) && tokenAddress != address(flip)
    );

    if (amount == 0) {
      amount = IERC20(tokenAddress).balanceOf(address(this));
    }

    IERC20(tokenAddress).transfer(owner(), amount);
}
```

CONTRACT INFO

Token Name Blastex token	Symbol BLASTX
Contract Address 0x5C598E410De1214D77EBB166102471065E7b2596	
Network Blast	Language Solidity
Deployment Date March 19, 2024	Contract Type Mintable token
Total Supply 1,000,000	Status Launched

TAXES

Buy Tax	Sell Tax
n/a	n/a

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	N/A
Uniq Senders	N/A
Uniq Receivers	N/A
Total Amount	N/A
Median Transfer Amount	N/A
Average Transfer Amount	N/A
First transfer date	N/A
Last transfer date	N/A
Days token transferred	N/A

SMART CONTRACT STATS

Calls Count	N/A
External calls	N/A
Internal calls	N/A
Transactions count	N/A
Uniq Callers	N/A
Days contract called	N/A
Last transaction time	Mar-19-2024 05:10:05 PM +UTC
Created	Mar-19-2024 04:58:59 PM +UTC
Create TX	0xa2f4835eccaa89b80c7e0a21302041b7e221e7ccf101d1bf1291b8d607e9b279
Creator	0x6d9725ffec14648300bc7bc6c9c0dd5ea631b39e

FOUND THREATS

⚠ High Risk

No high risk-level threats found in this contract.

⚠ Medium Risk

No medium risk-level threats found in this contract.

⚠ Low Risk

No low risk-level threats found in this contract.

FOUND THREATS

Informational

This token can be purchased only via the blasteX's staking contract. Owner can pause new buys 1 time before the launch of the platform.

```
bool public buyLocked = true;
function lockBuy() external onlyOwner {
    buyLocked = true;
}

function _beforeTokenTransfer(address from, address to, uint256 ) internal view override {
if (address(flip) == address(0) || !buyLocked) {
  return;
}

if (from == address(flip) || from == address(uniswapV2Router)) {
  require(
      to == mainContractAddress
    || to == address(uniswapV2Router)
    || to == address(flip)
    || to == address(0),
    "Transfer: only main contract can buy tokens"
  );
}
}
```

FOUND THREATS

Informational

New tokens can be minted only via the main (staking) contract.

```
function mint(address to, uint256 amount) public {
    require(msg.sender == mainContractAddress,
    "Mint: only main contract can mint tokens");

    _mint(to, amount);
}
```

Owner can set main (staking) contract once.
Main contract is set at address:
0x8C1DBB14c012bCCdB3477bc1625A3DCfD0F61ac2

```
function setMainContractAddress(address contractAddress) external onlyOwner {
    require(mainContractAddress == address(0), "Main contract address already configured");
    mainContractAddress = contractAddress;
}
```

According to their whitepaper:

BLASTX Distribution Model:

Bonding
Lock ETH for 5 to 30 days and receive a +5% to +30% bonus in BLASTX tokens.

Liquidity Staking
The transition from Bonding to Staking with profits capped at 150% to maintain perfect balance.

BLASTX Inflation Policy:

Unlimited Emission
Continuous incentives for Bonding and Liquidity Staking activities.

Controlled Inflation
Managed through Bonding, ReBonding, Liquidity Staking, and buyback-and-burning to ensure stability and resilience.

For more info, visit:
https://blastex.gitbook.io

TOKENOMICS

WEBSITE

Website URL
https://blastex.net/bonding

Domain Registry
https://namecheap.com

Domain Expiration
2025-01-04

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

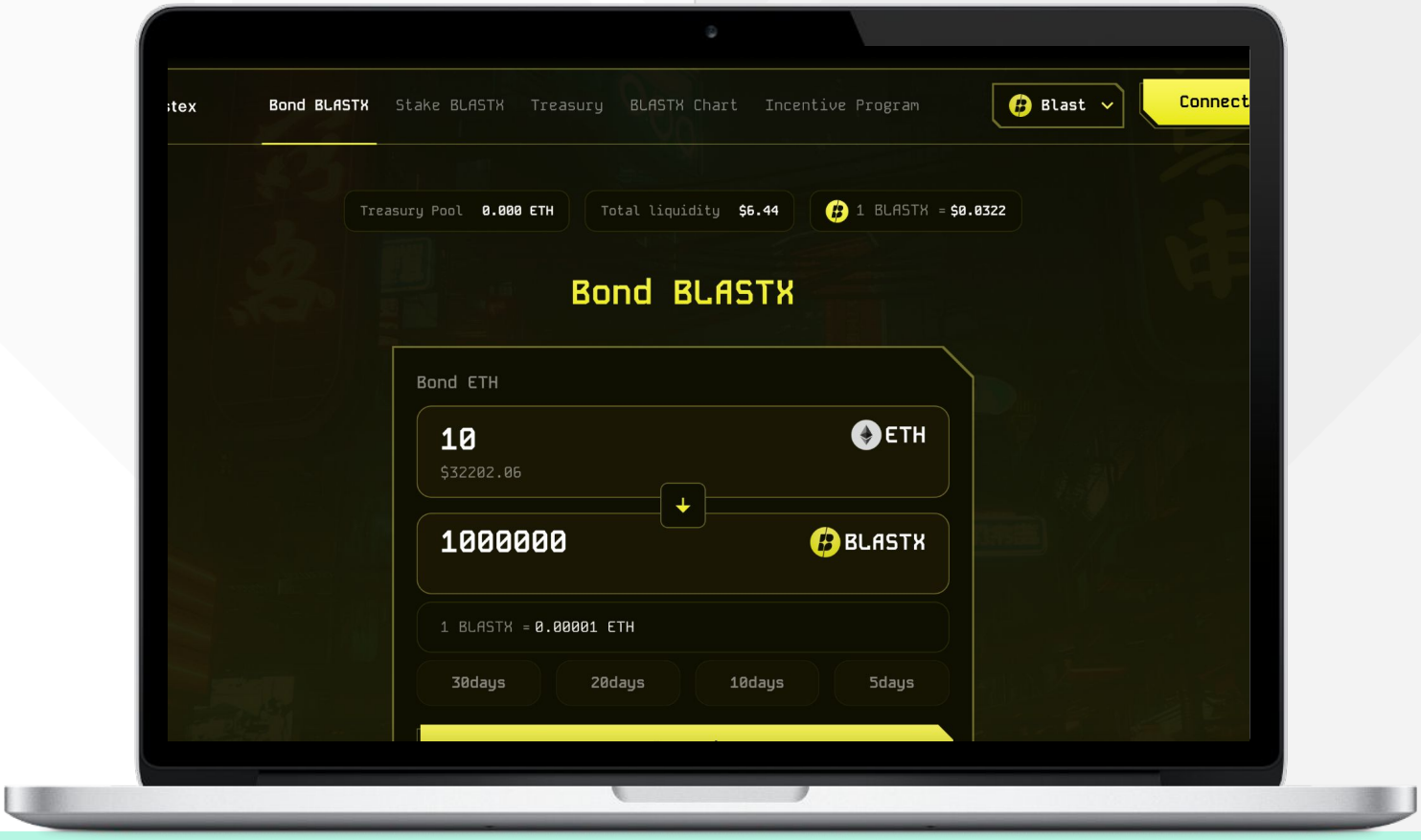
Design
Very nice design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written, informative.

Roadmap
No

Mobile-friendly?
Yes



blastex.net

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 700 SUCCESSFUL CLIENTS**
- **MORE THAN 1000 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.